UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/531,843	03/29/2007	Bernard Plessier	851663.479USPC	4061

30423 7590 09/29/2008

STMICROELECTRONICS, INC.
MAIL STATION 2346
1310 ELECTRONICS DRIVE
CARROLLTON, TX 75006

EXAMINER	
CHEN, SHIN HON	
ART UNIT	**PAPER NUMBER**
2131	

MAIL DATE	DELIVERY MODE
09/29/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/531,843	PLESSIER ET AL.	
	Examiner	Art Unit	
	SHIN-HON CHEN	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 August 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *8/14/07*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-21 have been examined.

Information Disclosure Statement

2. The information disclosure statement (IDS) submitted on 8/14/07 is being considered by the examiner.

Drawings

3. The subject matter of this application admits of illustration by a drawing to facilitate understanding of the invention. Applicant is required to furnish a drawing under 37 CFR 1.81(c). No new matter may be introduced in the required drawing. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d).

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1-21 are rejected under 35 U.S.C. 102(b) as being anticipated by Dworkin et al. U.S. Pub. No. 20020066014 (hereinafter Dworkin).

6. As per claim 1, Dworkin discloses an apparatus arranged to accept digital data as an input and to process the data according to one of either the Secure Hash Algorithm (SHA-1) or

Message Digest (MD5) algorithm to produce a fixed length output word (Dworkin: [0009]: Message Digest Accelerator implements algorithms like MD5 and SHA), the apparatus comprising:

a plurality of rotational registers for storing data, one of said registers arranged to receive the input data (Dworkin: figure 1: registers A-E; [0011]); and

data stores for initialization of some of said plurality of registers according to whether the SHA-1 or MD5 algorithm is used, said data stores including fixed data relating to SHA-1 and MD5 operation (Dworkin: [0011]: the register files store values for initialization); and

a plurality of dedicated combinatorial logic circuits arranged to perform logic operations on data stored in selected ones of said plurality of registers (Dworkin: [0012]: function circuit performs logical operations on the registers).

7. As per claim 2, Dworkin discloses the apparatus of claim 1. Dworkin further discloses wherein the register arranged to receive the input data is arranged to receive said input data serially (Dworkin: [0010]: MDHA takes input text message and breaks it into blocks for parallel processing).

8. As per claim 3, Dworkin discloses the apparatus of claim 1. Dworkin further discloses wherein the registers and combinatorial logic circuits are interconnected for communication via a pair of data busses (Dworkin: figure 1: architecture of the MDHA).

9. As per claim 4, Dworkin discloses the apparatus of claim 3. Dworkin further discloses wherein the registers and combinatorial logic circuits are connected to write to a respective bus via respective tristate buffers (Dworkin: [0014] lines 22-24: the tristate buffers select the register files).

10. As per claim 5, Dworkin discloses the apparatus of claim 1. Dworkin further discloses wherein the apparatus includes a control circuit arranged to generate individually gated clock signals for each register (Dworkin: [0011]: the register file values are altered on every clock cycle generated by the control circuit).

11. As per claim 6, Dworkin discloses the apparatus of claim 5. Dworkin further discloses wherein said control circuit is further arranged to generate individual enabling signals to control the tristate buffers (Dworkin: [0014] lines 22-24: the control circuit manages clock cycle and the tristate buffers).

12. As per claim 7, Dworkin discloses the apparatus of claim 1. Dworkin further discloses wherein the rotational registers are arranged to be multiplexed prior to connection to a tristate buffer (Dworkin: [0014] lines 22-24: multiplexer functions; [0019]).

13. As per claim 8, Dworkin discloses the apparatus of claim 1. Dworkin further discloses wherein the combinatorial logic circuits include a copy circuit, a shift left circuit, a NOT circuit,

an ADD circuit, an OR circuit, an AND circuit and an XOR circuit (Dworkin: figure 1 and [0012]-[0014]).

14. As per claim 9, Dworkin discloses the apparatus of claim 1. Dworkin further discloses wherein the apparatus is implemented as an integrated circuit (Dworkin: figure 1 and [0009]: hardware accelerator with integrated circuits to generate secure message digest).

15. As per claim 10, Dworkin discloses the apparatus of claim 1. Dworkin further discloses wherein the apparatus further includes circuitry arranged to perform digital signature creation or authentication (Dworkin: [0009]: well known algorithms for generating digital signature and authentication).

16. As per claim 11-21, claims 11-21 encompass the same scope or obvious variation of claims 1-10. Therefore, claims 11-21 are rejected based on the same reasons set forth above in rejecting claims 1-10.

Conclusion

17. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Jain U.S. Pat. No. 6300791 discloses signature generator integrated circuit that takes words in series and process them in parallel fashion to generate signature.

Smith et al. U.S. Pub. No. 20010001155 discloses method for providing public key security control for a cryptographic processor.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SHIN-HON CHEN whose telephone number is (571)272-3789. The examiner can normally be reached on Monday through Friday 8:30am to 5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Shin-Hon Chen
Examiner
Art Unit 2131

/Shin-Hon Chen/

Examiner, Art Unit 2131